



# Trendspek

## Trust & Assurance

## Trendspek Compliance Overview

[trendspek.com](https://trendspek.com)

This Document must not be reproduced, in whole or in part, without the prior written consent of Trendspek.

# Compliance Overview

## Summary of Contents

### Page 3

#### Executive Summary

### Page 4

#### Compliance

- ISO 27701 Privacy Management
- ISO 9001 Quality Management
- PCI/DSS
- EU GDPR
- Security of Critical Infrastructure Act

### Page 5

#### Cybersecurity

- SOC 2 Type 2
- ISO 27001 Information Management

### Pages 6-7

#### Infrastructure and Cloud

- Data Encryption Data Backups Data
- Availability Physical Access Cloud
- Service Providers Penetration
- Testing Sub-Processors

### Page 8

#### Infrastructure

### Page 9

#### Privacy

- Data Sovereignty
- Data Residency
- Data Retention
- EU GDPR and ISO27701
- Privacy Policy
- Privacy Officer

### Page 10-12

#### Application Security

- Login Security Single Sign-On (SSO)
- Single Sign-On (SSO)
- Access Control: RBAC & Permissions
- User Lockout
- Password policy
- Change Management
- User Logs
- Incident notification
- Data Handling

### Page 13

#### Corporate Security

- Office Security Workstation and Mobile Management
- People Management

### Page 14 - 15

#### Data Acquisition Security

- Data Acquisition Workflow

### Page 16

#### Policies and Statements

- Information & Data Security Policy
- Acceptable Use Policy Technical
- Support Service Policy Quality
- Policy Privacy Policy Cookies
- Consent Modern Slavery
- Statement Workplace Health and
- Safety Policy ESG Statement

### Page 17-18

#### Appendix 1.1

#### Appendix 1.2

### Page 19

#### Contact Information

# Executive Summary

At Trendspek, protecting your data is paramount to us. We are dedicated to safeguarding your data and information through rigorous security and compliance measures, and ensuring that we maintain global-leading accreditations.

## Our Commitment

- SOC2: Trendspek has SOC 2 Type 2 attestation, a robust cybersecurity audit assessing an organisation's cyber controls at a single point in time and within a prescribed time period to safeguard organisational, customer data, and sensitive information.
- ISO 27001 ISMS: As one of the few providers in our class of software to achieve this certification, we adhere to the highest standards for Information Security.
- ISO 27701 PIMS: Trendspek is certified for Privacy Information Management Systems, meeting international security and privacy standards, including compliance with European GDPR requirements.
- ISO 9001 QMS: Our commitment to quality is reflected in our certification for Quality Management Systems, ensuring excellence in our service and products

## Auditing and Compliance

Trendspek undergoes continuous external auditing and surveillance to maintain our ISO certifications, reinforcing our commitment to cybersecurity best practices. Additionally, we hold SOC 2 Type 2 attestations, which evaluate our cybersecurity controls and protect both organisational and customer data.

## Privacy and Data Protection

With our ISO 27701 Privacy Information Management System certification, we meet rigorous GDPR privacy standards, demonstrating our dedication to protecting personal information.

## Proactive Security Measures

To enhance our security posture, we collaborate with leading providers of cybersecurity services, to conduct regular penetration testing of our software. Furthermore, we utilise PCI/DSS compliant providers to ensure secure payment processing for our clients.

Trendspek remains committed to maintaining the highest standards of cybersecurity to protect our clients and their data ensuring confidentiality, integrity and accessibility of your data.

The Trendspek logo is displayed in white text on a dark, diagonal background element that overlaps the bottom left corner of the page. The logo consists of the word "Trendspek" in a bold, sans-serif font, with a small red and white graphic element above the letter 'k'.

The 3D software that **transforms** structural lifecycle management.

The following security-related audits, certifications, regulations apply to Trendspek:



## ISO 27701: Privacy Information Management System [PIMS]

Trendspek is committed to meeting and exceeding international security, quality and privacy standards including European GDPR and the Australian Privacy Act compliance requirements. Trendspek is certified to ISO27701 PIMS [Privacy Information Management Systems].



## ISO 9001: Quality Management System [QMS]

Trendspek is committed to the quality of our service and our product and is certified to ISO 9001 QMS [Quality Management Systems].



## EU GDPR

Trendspek is compliant with European General Data Protection Regulation (GDPR) requirements for customer information privacy standards and is certified for ISO27701 PIMS [Privacy Information Management System].



## PCI/DSS

Trendspek's payment and credit card information is handled by Stripe. Stripe have been audited by an independent PCI Qualified Security Assessor (QSA) and are certified as a PCI Service Provider Level 1. This is the most stringent level of certification available in the payments industry.



## Security of Critical Infrastructure Act (SOCi)

Trendspek is compliant with the Security of Critical Infrastructure Act 2018 (SOCi), the Commonwealth of Australia's framework for managing risks relating to critical infrastructure.

The following security-related audits, certifications, regulations apply to Trendspek:



## ISO 27001: Information Security Management System [ISMS]

Trendspek is certified to ISO27001 for Information Security. Trendspek undergoes constant external auditing and surveillance as part of its ISO 27001 certification. All policies, procedures and risk registers are formatted to ISO 27001 standards.



## SOC 2 Type 2

Trendspek has received SOC 2 Type 2 compliance attestation, a robust cybersecurity audit assessing an organisation's internal cyber controls and systems within a prescribed time period related to security, availability and confidentiality of data.

## Data Encryption [In Transit and At Rest]

Trendspek uses best-practice authentication and encryption in transit and at rest. Data in transit is secured with SSL. AWS RDS Database / Azure Database is encrypted at rest using industry-standard encryption algorithms. AWS S3 / Azure Blob storage is encrypted at rest using industry-standard encryption algorithms. All servers and other stores of data have encrypted root volumes.

## Data Backups

In the unlikely event of customer data loss, procedures and safeguards are in place to ensure recovery. The majority of customer data is stored in Amazon's S3 which is rated to have 99.999999999% durability.

Database snapshots are taken every 24 hours and stored across multiple availability zones. Data (models, images) backup and integrity are managed by AWS S3 and Azure Blob. In the event of a disaster, AWS and Azure would manage the recovery and restoration of lost data.

## Data Availability

AWS and Azure are well known for their stability and reliability. Nevertheless, outages can occur in exceptional circumstances. If an outage occurs, a technical member of staff will endeavour to resolve the issue as quickly as possible. Trendspek endeavours to maintain a 99% yearly uptime.

## Physical Access

All services are contained within Trendspek's virtual private cloud with no public access possible. Trendspek Cloud infrastructure is private and isolated with restricted access to the internet. Data is accessible via cloud to the nearest cloud region available to the user. Trendspek's data is segmented from other user data in the cloud.

## Cloud Service Providers

Trendspek is hosted on the Amazon Web Services (AWS) platform, Google Cloud and Microsoft Azure platforms (Private Instance only).

AWS, Google Cloud and Azure provide state-of-the-art data centre security that complies with industry standards such as SOC, PCI DSS, and ISO 27001. All physical network and server security responsibility are delegated to the cloud provider.

For more information regarding AWS's security practices, check out [their security whitepaper](#).

For more information regarding Azure's security practices, check out [their security whitepaper](#).

For more information regarding Google Cloud's security practices, check out [their security whitepaper](#).

# Infrastructure & Cloud

## Penetration Testing

Trendspek is also subject to external penetration testing and internal auditing. This is performed at least annually.

## Sub-processors

Entity Name	Sub-processing Activities
Amazon Web Services, Inc.	Cloud service provider (Current, Primary)
Azure	Cloud service provider (Available Upon Request)
Google Cloud Platform	Cloud service provider (Available Upon Request)
Intercom	Customer support platform
Hubspot	Customer Relationship Management (CRM)
Peakhour	Content Delivery Network (CDN)
Posthog	In-app analytics
New Relic	Application monitoring
Stripe, Inc.	Payment processing
Stytch	Identity Provider (IdP)



## Data Sovereignty

Data is subject to the laws of the geographic location where data is collected and processed. Data is held in Trendspek in accordance with client agreement.

## Data Residency

Trendspek primarily operates in AWS Sydney, with the ability to store data in other regions to suit customer specific requirements.

AWS: Users have access to [AWS servers globally](#), in accordance with their commercial agreement and aligned to their regional requirements.

Azure: Users have access to [Azure servers globally](#), in accordance with their commercial agreement and aligned to their regional requirements.

Google Cloud (Sydney Australia Server) is utilised for processing customer data.

## Data Retention

Trendspek is transparent about the data in use and allows users to take full control of information collected, including models, annotations and PII. Users can request to remove data in accordance with Trendspek's [Privacy Policy](#).

## EU GDPR and ISO27701

Trendspek is compliant with European General Data Protection Regulation (GDPR) requirements for customer information privacy standards and is certified for ISO27701 PMS [Privacy Information Management System].

## Privacy Policy

Trendspek's Privacy Policy explains how we collect, use, and share personal information, including name, contact details, and usage data, to enhance our services. Users have rights under GDPR, including access, updates, and opting out of data collection, though opting out may limit service access.

[Read Trendspek's Privacy Policy](#).

## Privacy Officer

Mitch Deam  
Trendspek Operations Pty Ltd  
Suite 1.103/477 Pitt St, Haymarket NSW 2000  
Email: [compliance@trendspek.com](mailto:compliance@trendspek.com)

# Application Security

## Login Security

Trendspek uses an IaaS provider with Multi-factor authentication and encryption of data-at-rest and in-transit. The identity provider is HIPAA eligible and PCI DSS, SOC, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and ISO 9001 compliant.

## Single Sign-On (SSO)

Trendspek supports Single Sign-On (SSO) to streamline secure access for organisations. Integration is available via SAML or OIDC, enabling authentication through existing directory services. SSO simplifies user access, supports centralised access control, and helps meet internal security and compliance requirements. SSO configuration is available upon request as part of supported access options.

## Access Control: RBAC & Permissions

Trendspek implements Role-Based Access Control (RBAC) to ensure users are granted the minimum permissions required for their responsibilities. Roles are assigned based on job function, and permissions are granularly scoped within the platform. Admin roles can manage user access, review activity logs, and enforce security configurations. This approach strengthens internal data governance and protects sensitive information from unauthorised access.

## User Lockout

Session will time out after a determined period of time. Trendspek typically starts denying your login attempts after a determined number of rapid login attempts, or rapid login attempts from varying locations. A user will be entirely disabled if a brute force attack is sensed.

## Password Policy

Password standards are set by Trendspek and must be a complex password with a minimum character length inclusive of other requirements set by NIST 800-63.

Passwords are able to be reset via the dashboard or login page. Access to users email is required if resetting through the login page in order to obtain authorisation codes. Trendspek does not have access to users' credentials.

Multi-factor authentication (MFA) may be used to provide additional security, with access codes sent to the user's device.

# Application Security

## Change Management

As a web application, code changes are made and deployed in a continuous manner with an internal versioning system. Majority of updates are conducted at off-peak times. No action is required to update to the latest version beyond refreshing the browser.

## Incident notification

Trendspek will notify relevant users without undue delay of any suspicious activity or data breaches regarding Trendspek and or user data, as set out in its Security policy and procedures manual.

## User Logs

Trendspek maintains administration and end-user logs to provide an audit trail and to enable quick investigation of potential threats or issues.

Every interaction between Trendspek Infrastructure and an end-user is logged on a granular level. Trendspek captures all traffic specific to the network - any traffic going through the endpoints will be captured, as will any admin CLI or web console activity.

Some information that may be logged includes IP addresses, request headers, request payloads, device information, status codes, response times, and failed login attempts. We never log confidential or sensitive data.

Trendspek's logs are accessible by only a few key Trendspek staff. They are encrypted at rest and stored for 365 days.

## Secure SDLC

The application is developed securely according to OWASP Top 10 guidelines. All source code is scanned with SAST / DAST tools through our CI/CD pipeline. There are rigorous controls in place around the review, QA, and releasing application updates.

# Application Security

## Data Handling

Trendspek's platform manages high-resolution asset data and client content that may be sensitive or commercially confidential. Secure and compliant handling of this information is essential to meet regulatory requirements, support client expectations, and ensure operational integrity.

### Why This Matters

Any incident involving data mishandling—no matter how minor—can lead to:

- Reputational damage and loss of client trust
- Delays in project delivery or decision-making
- Breaches of legal and contractual obligations

Secure data handling ensures that content hosted on the Trendspek platform is protected, reliable, and managed responsibly throughout its lifecycle.

## Handling Guidelines

### Secure Transfer

All content uploaded to Trendspek is transferred via encrypted HTTPS channels to safeguard against interception and tampering.

### Access Control

Access to data is managed through Trendspek's Role-Based Access Control (RBAC) system. Only authorised users can access content, based on their role and assigned permissions.

### Data Retention and Disposal

Data retention requirements vary by client and jurisdiction. Trendspek follows the data handling instructions provided by clients and ensures:

- Secure deletion of data when no longer required
- Removal of content from backups in line with internal policies
- Alignment with AWS and Azure's data disposal standards

### Regulatory Compliance

Trendspek complies with applicable privacy laws, including the Australian Privacy Act and other statutory or industry-specific obligations as required.

### Client-Specific Requirements

Some projects may involve additional requirements, such as limited access, data localisation, or shorter retention periods. These are captured at the outset of the project and enforced throughout.

## Data Checklist

- Upload content via secure HTTPS connection
- Ensure data is associated with the correct project
- Restrict access to authorised users only
- Follow any client-specific data handling requirements
- Adhere to internal or client-defined retention timelines
- Request secure deletion when content is no longer needed
- Immediately report any suspected data handling issues

# Corporate Security

## Office Security

Trendspek offices are secured with self-closing, self-locking doors with access managed via electronic tags. Access is recorded and entry logs are maintained. The offices are also secured with security access gates, and all areas are monitored by CCTV security cameras.

## Workstation and Mobile Management

All devices used by our staff members are required to be password protected, with automatic locking after short periods of disuse in addition to full-disk encryption. Devices are monitored and can be remotely wiped in the event of a breach. Enabling MFA for online access is a mandatory policy for all staff.

## People Management

### Internal training

All Trendspek team members conduct continuous internal training throughout the course of their employment.

Internal training during onboarding covers all aspects of the Trendspek platform and supporting infrastructure, including dedicated onboarding for compliance and cybersecurity process and procedures.

Trendspek team members complete ongoing and continuous training to ensure that team members are up to date with the latest processes and procedures.

### Security clearance checks (Employees)

All Trendspek team members are subject to thorough hiring processes, which include mandatory police and government security checks.

# Data Acquisition Security

## Secure Drone Teams: End-to-end

Trendspek recognises and supports the compliance requirements for the purpose of data acquisition using robotics and drones.

Trendspek provides further recommendations to Capture Providers to reduce risk and improve efficiency, including:

1. Robust analysis of the data acquisition process on a case-by-case basis.
2. Use of appropriate data shredding processes.
3. Data storage and retention processes.
4. Use secured network to upload data files to Trendspek's data processing software.
5. Ensuring our providers are operating in accordance with manufacturer security protocols.
6. Providing data acquisition teams a secure method of uploading data to Trendspek's servers

## Handling of Drone-Captured Data

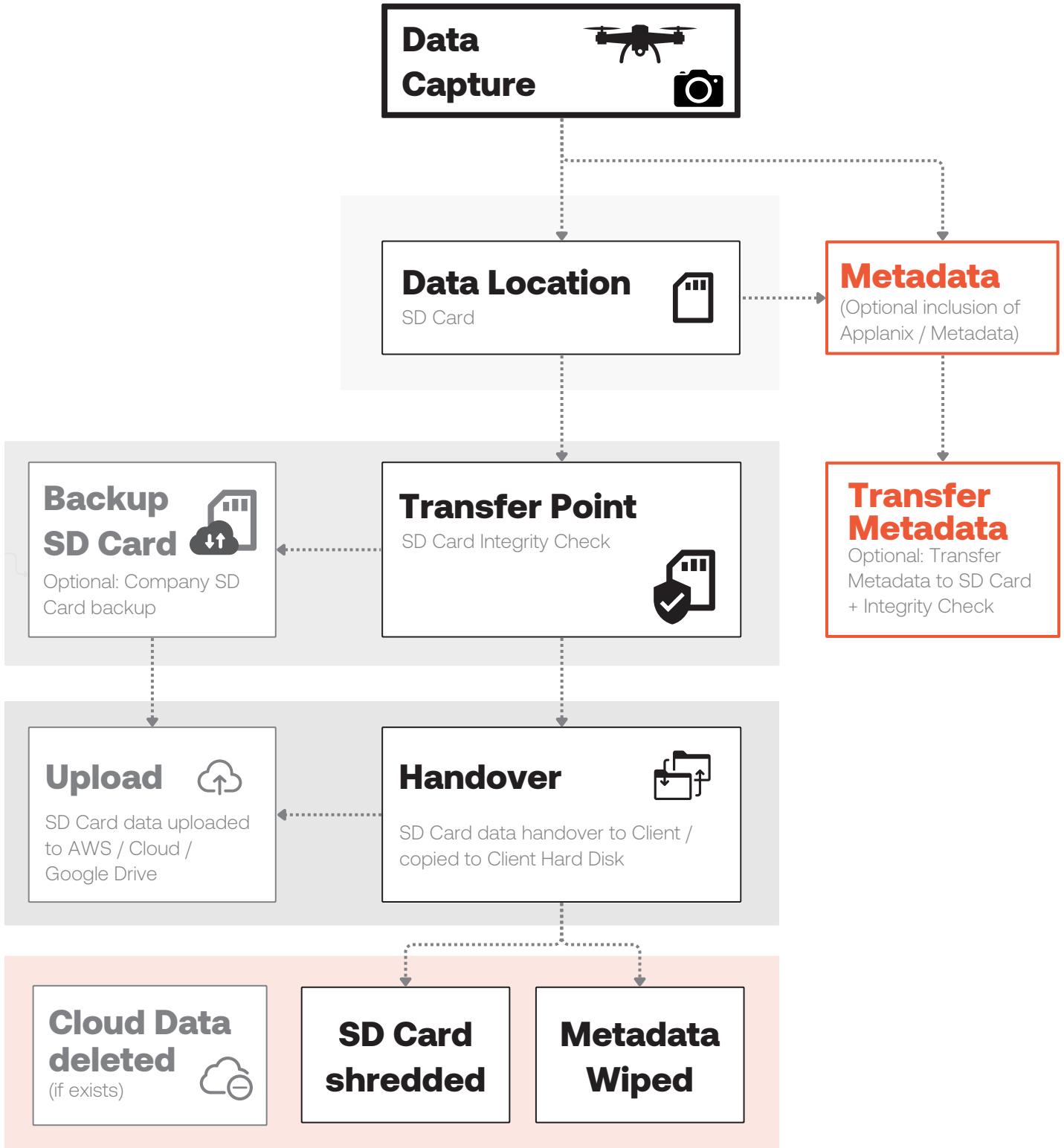
Drone-captured data often includes high-resolution imagery and sensitive operational details.

Trendspek applies its standard data handling practices to this content, including encrypted HTTPS transfer, strict access control, and secure disposal aligned with client and legal requirements.

These controls ensure that even externally captured data is managed in line with our broader information security and compliance framework.

# Data Acquisition Security

## Data Acquisition Workflow



# Policies and Statements

## **Information & Data Security Policy**

[Information & Data Security Policy](#)

## **Acceptable Use Policy**

[Acceptable Use Policy](#)

## **Technical Support Service Policy**

[Technical Support & Service Level Policies](#)

## **Quality Policy**

[Quality Policy](#)

## **Privacy Policy**

[Privacy Policy](#)

## **Cookies Consent**

[Cookie Consent](#)

## **Modern Slavery Statement**

[Modern Slavery Statement](#)

# Appendix 1.1

## ISO 9001:2015 Quality Management System Certificate

Date of issue: 1 June 2020 Date of reissue: 17 July 2023  
 2023 Expiry Date: 01 June 2026 Audited and certified by ISOQAR



## ISO 27001:2022 Information Security Management System Certificate

Date of issue: 1 June 2020 Date of reissue: 2 June 2025  
 Expiry Date: 01 June 2026 Audited and certified by ISOQAR



## ISO 27701:2019 Privacy Information Management System Certificate

Date of issue: 17 July 2023 Date of reissue: 2 June 2025  
 Expiry Date: 01 June 2026 Audited and certified by ISOQAR



# Appendix 1.2

## SOC2 Type 2 Certificate

Date of issue: May 15 2025

Assessment period: April 16 2024 - April 15 2025

Audited and certified by Accorian Assurance



# Our Compliance Team



**Mitch Deam**  
**Chief Compliance Officer**  
Trendspek  
[mitch@trendspek.com](mailto:mitch@trendspek.com)



**Amith Raj**  
**Head of Cybersecurity**  
Trendspek  
[amith@trendspek.com](mailto:amith@trendspek.com)



**Romanille Salvador**  
**Junior Security Analyst**  
Trendspek  
[romanille.salvador@trendspek.com](mailto:romanille.salvador@trendspek.com)

**Contact Trendspek's Compliance Team:**  
[compliance@trendspek.com](mailto:compliance@trendspek.com)

**Trendspek**

[trendspek.com](https://trendspek.com)

This Document must not be reproduced, in whole or in part, without the prior written consent of Trendspek.